CRS Build 11.0/VIP Build 3.2 Release Notes

These notes document the new features and bug fixes incorporated into the CRS Build 11.0 and VIP Build 3.2 software releases. Trouble Ticket Request (TTR) numbers have been provided to reference formally documented problems that have been resolved by this build. The following TTRs are listed numerically in two categories: Software enhancements and bug fixes.

SOFTWARE ENHANCEMENTS - CRS

1. **TTR 892: CRSSITE Cleans Out Activity Logs** – The CRS_SITE utility takes a database ASCII file and loads the database and system configuration. The Activity Logs contain two logs: the Transmit Log and the Error Log. The Transmit Log contains an archive of all messages transmitted on all transmitters, including SAME and Alert Tone information. The Transmit Logs are contained in the database tables directory in files named LGYYMMDD.dat and LGYYMMDD.idx0, where YY = Year, MM=Month, and DD=Day. The Error Logs are named ERYYMMDD.dat and ERYYMMDD.idx0. Prior to CRS Build 11.0, when XCRS_SITE was run to reload the system configuration and the database, these files were wiped clean. This would destroy the archive of the activity log, including the transmit log, which may be needed to prove that warning messages were transmitted.

   New options have been added to CRS_SITE to allow the Transmit and Error tables to remain unchanged, similar to what was done for the dictionary tables. The default for the dictionary files is to leave them unchanged. This will also be the default for the Transmit and Error logs.

2. **TTR 911: CRS Only Looks For AS And DS AWIPS Platforms** – CRS checks for AWIPS connectivity at initialization and every 30 minutes thereafter. If no AWIPS processor is found on the network, CRS generates a high priority alert monitor message indicating the AWIPS interface is down. Also, the found AWIPS processor is used once a day to for time synchronization. Therefore, if no AWIPS processor is found, time synchronization with AWIPS will not occur.

   Prior to CRS Build 11.0, CRS would look for the AS1, AS2, DS1, and DS2 AWIPS processors, depending on which of these were placed in the /etc/hosts file. The AS and DS platforms are being removed as part of AWIPS planned platform upgrades. Therefore, a better CRS procedure must be designed to handle new AWIPS platforms.

   The CRS software has been modified to handle new AWIPS platforms. A new AWIPS Authorization file has been created that contains multiple AWIPS platform entries. The CRS_SITE utility has been modified to use the first processor found in the AWIPS Authorization file as the AWIPS network rather than the first entry (AS1) in the /etc/hosts

file. The AWIPS network address is stored in shared memory and retrieved when determining if AWIPS communications are available. The AWIPS communications checks in the CP_AI module have removed the extraction of the AWIPS hosts from the /etc/hosts file and use the AWIPS Authorization file in its place. If the current processor is deemed inaccessible, the AWIPS Authorization file is used to retrieve the next available processor. The order of AWIPS processors in the AWIPS Authorization file is PX1, PX2, DX1, DX2, DS1, and DS2. This modification was implemented as CRS patch 10.0.1.

3. **TTR 914: Add Error And Transmit Database Table Deletion To XCRSSITE GUI** – See TTR 892. With the addition of the new options to leave unchanged the Error and Transmit logs when the database is loaded, the XCRSSITE utility has added a new option on the left side of the window to allow the user to delete the Error and Transmit logs. The default selection for the new option is to leave intact the old transmit and error logs. Alternatively, if the operator so chooses, he/she may wipe out the transmit and error logs. This new option is only applicable if the operator is initializing the database and system configuration.

4. **TTR 930: CP_DI_ADC Logging** – With the implementation of threading in CP_DI_ADC, a new logging implementation required the use of a configuration file to set the log level. However, the logging software does not allow the log level to be retrieved from the system setlog configuration file.

   Build 11.0 allows the log level to be retrieved from the setlog configuration file.

5. **TTR 932: Add Site Configurable Tone Validation Warning To EO Transmit** - Currently, the CRS software contains a site configurable Tone Validation (Maintenance Menu, Site Configuration, Interface tab) option that when selected will cause a warning to be displayed whenever the operator attempts to save a message via the Weather Message window for which SAME and/or Alert tones have been selected. The operator must either select “OK” to save the message or “CANCEL” to cancel the save action.

   Build 11.0 modifies the Emergency Override (EO) window software to check for Tone Validation activation to determine if the same warning message is to be displayed when the EO Transmit button is selected. Therefore, if a site has activated the Tone Validation option, the warning message always will be displayed for Weather Message window generated messages containing tones and all EO transmissions. Also, the warning message has been modified to include the Message Type Title, i.e. Santa Barbara Tornado Warning. Software Note 11, which will contain the detailed CRS software installation instructions, will contain directions for sites to check the Tone Validation parameter and to set as determined by their specific operational requirements.

SOFTWARE ENHANCEMENTS – VIP

1. **TTR 906: Add Product Filter To VIP Remote SFTP** – The VIP remote sftp function allows sites to send voice files, either .wav or .mp3, to an external system. Prior to VIP Build 3.2, the VIP remote sftp function included all voice files processed by VIP for CRS scheduling and subsequent broadcast on NWR. There was no way to filter out unwanted messages or to define a subset of messages for remote sftp processing.

   With the approval of CRS Request for Change AC433 (WRH347), the VIP software has been modified to define a filter that allows sites to select specific Message Types for routing to the external system. The VIP main menu contains a new option (Remote Product Filter) in the File pull-down menu. When selected, the Remote Product Filter window appears and allows the user to add/delete specific Message Types. The remote sftp function only occurs for those Message Types contained in the Remote Product Filter list. Since sites must specify the exact 9-character Message Types that will be used for the remote sftp function, Software Note 11 will contain directions for sites to populate the Remote Product Filter list.

BUG FIXES – CRS

1. **TTR 847: UnixWare Warning Message That MEMFS Virtual File System Is Filling UP** - A message similar to the following may appear in the Message Monitor (MMI):

   MMI(9387): WARNING: Volume /usr/merge/memfs low threshold of 20.0% reached at 45.54 or 258.93 MB free (17.59%

   The /usr/merge/memfs is a virtual file system using RAM as its storage area. It is designed for fast access and allows Windows to run under UnixWare. It enables the user to perform various windows related commands such as mcopy, mdir, etc. Over time, the space may start to get used up if you have not done a Master MP operating system reboot in a while. The warning message is merely stating that this file system is filling up and the system should be rebooted before too long, or the system can completely lock up. If you open a Unix shell and try to list the contents of the file system via the ls -l command, no files will be listed. Do not be confused by this; if you enter the df -k command, the system will list the amount of space used and remaining for all file systems. The warning is programmed to occur when you have used up 80% of the space allocated to the file system. It will probably take several months from the last Master MP reboot before you will get this message. Since you still have 20% of the space remaining, there is no immediate need to reboot the Master MP, but you should plan on doing it within a couple of days. You will continue to receive periodic MMI warning messages, so you can see how close you are to running out of space. Prior to CRS Build 11.0, the operating system configurable parameter for this virtual file system was set to 10 megabytes.

The CRS software has been modified to double amount of space for the memfs virtual file system to 20 megabytes.

2. **TTR 865: Default Directory On The Weather Message Correction Did Not Contain A Message With An Error** - Prior to CRS Build 11.0, if a message with a bad expiration time was received from AWIPS, the bad message was not placed in the correct error directory, i.e. the message was placed in the /crs/data/CP/VC directory instead of in the /crs/data/CP/VC/error directory. The problem was that messages that fail the message header validity check before being assigned for processing by either DECTalk or VIP remain in its default processing directory. For VIP messages this is the /crs/data/CP/VC directory.

   The CRS software has been modified to redesign the verify message function so it now processes all validation procedures before moving the weather message into the default processing directory.

3. **TTR 876: CRS Performed Diagnostic Test On A Non-Existent Transmitter** – Prior to CRS Build 11.0, when ACP diagnostic tests were performed on the ACP2 for a Large 7 system, on the 4th diagnostic step, when the system was cycling back from PB2 to the Transmitter #1, it cycled through the Transmitter #13 (which is a non-existence transmitter) and then to Transmitter #6 though Transmitter #1.

   The Communications Processing software that processes ACP input signals (CP_PI) has been modified to correct the problem with processing diagnostic information in the Large 7 configuration.

4. **TTR 878: CRS Shutting Down During MP Switch-Over** - Prior to CRS Build 11.0, under certain conditions, during a Main Processor (MP) switch-over, the database validation and verification (DB_VV) process shuts down and restarts repeatedly, thereby preventing a successful start of the CRS application software. This problem would only occur a small percentage of times, because of the timing involved. The problem required that all configured FEPs report immediately. The problem was with the shadow control process (SS_SH), which sets the show MP status to enabled=false and synchronized=false. This configuration along with shadow processor status being down is identical the backup MP being offline. This confusion results in the algorithm that determines if the CRS is operational to fail, since the FEP processors become operational immediately, and the assumed status for the shadow MP is offline.

   CRS Build 11.0 eliminates the confusion between whether the shadow MP is online or simply has not finished initialization and when the shadow is actually offline, by defining a new variable that determines whether or not the shadow is supposed to be enabled.

5. **TTR 879: Message Type Deletion Error** - Prior to CRS Build 11.0, deleting a Message

Type resulted in an extraneous record being kept in the database. This caused no operational impacts other than a "Data Verify failed: No Message Type associated with this record MessageDateTable [xxx yyy]" error message, where xxx is the Message Type number and yyy is the version number of the message.

CRS Build 11.0 removes the extraneous record when the Message Type delete is performed, thereby eliminating the Data Verify error.

6. **TTR 880: SSO VIP Retry Leaves Shadow File Undeleted** - Prior to CRS Build 11.0, Synthetic Speech Override (SSO) messages that the operator selected for VIP Retry were correctly processed and removed from the SSO message list. However, even though the raw SSO message had been deleted from the /crs/data/CP/sso directory on the Master MP, it was not deleted from the Shadow MP directory.

   Build 11.0 removes the SSO message from the Shadow MP directory.

7. **TTR 883: The FTP.KSH File Still Contains "FTP" Remarks In Its Comment Lines** - Prior to Build 11.0, several old references to the old ftp command that was replaced with sftp in Build 10.0 were left in comments in the ftp.ksh script.

   The comments in the CRS Build 11.0 ftp.ksh script no longer reference ftp.

8. **TTR 884: CP_AI_RCV Terminated Multiple Times Overnight** – Prior to CRS Build 11.0, it was possible to occasionally have the AWIPS Input Receive process (CP_AI_RCV) fail. The process would immediately restart, no data was lost, and other than an error message appearing in the Alert Monitor, no negative impact was detected. This problem was caused by a signal race condition which happened when a second signal occurred while the signal handler function was being executed. This caused the processing of the default action of the second signal, and CP_AI_RCV exits.

   In CRS Build 11.0, the possibility of a signal race condition has been reduced by using a sigaction to initialize the signal handler, which allows us to block the SIGUSR1 signal and process the other one.

9. **TTR 886: WRSAME Tone Generator Save/Restore Settings Problems** – Prior to CRS Build 11.0, sites could experience the following scenario. An operator used the WRSAME Tone Generator window to change tone amplitudes. Before changing any of the amplitudes, he/she used the WRSAME Tone Generator window to save the current settings. Then new amplitudes were entered and saved. Then CRS was stopped and restarted. When the NWRSAME Tone Generator was displayed, the original saved values were restored and saved. The problem was the old values did not get restored under this scenario. The reason they did not get restored is WRSAME Tone Generator software read the data from the restored file correctly, but did not force the GUI amplitude slider bar to reflect the value from the restored file.

The WRSAME Tone Generator software in CRS Build 11.0 forces the amplitude slider bar to move according to the latest amplitude value read from the restored file.

10. **TTR 893: ROAMS More Window Displays Bad Machine Password** – Prior to CRS Build 11.0, it was possible to display garbage following the correct display of the machine password in the ROAMS MU data display. The problem was that sometimes the password string did not terminate with a NULL character prior to being displayed.

    CRS Build 11.0 always appends a NULL character to the last character of the password string.

11. **TTR 910: CP_DI_ADC Retry Transmission Does Not Seek New Position Properly** – CP_DI_ADC performs a streamcopy function to move completed VIP wave files from the Master MP to all other processors. Prior to CRS Build 11.0, if the streamcopy software needed to retransmit the data due to a packet error, the retransmission would fail, causing a retry of the streamcopy function by CP_VC. This streamcopy retransmission failure is used by a read function failure resulting from an invalid value for the file descriptor variable being passed. The value is that of the microphone and not the VIP component file.

    This problem has been fixed in CRS Build 11.0 by passing the correct file descriptor variable, so that CP_DI_ADC can handle the error processing instead of CP_VC.

12. **TTR 916: Add New Key West Site Identifier to CRS** – The Key West office is moving to another location on the island, which requires changing the site identifier from KEYW to KKEY. The correct site identifier must be entered when a new software Build is installed. The SITE_INFO file has been changed to add KKEY to the file.

13. **TTR 918: OverrideDefined Option Prevents User From Setting Listening Areas During Manual Weather Message Creation** – The CRS Message Type software contains a Listening Area Override parameter. When this parameter is selected, the message processing software will ignore the Listening Areas on the incoming AWIPS messages and instead use the default Listening Areas stored in the CRS database as part of the Message Type definitions. The problem occurs for manually recorded messages (Emergency Override or Weather Message Record). In this case if the operator modifies the default Listening Areas to something else, the software allows these to be saved, but ignores the changes. Instead, it uses the default Listening Areas, as if the operator had made no changes. This may result in a warning message being broadcast on the wrong transmitters.

    To correct this problem, CRS Build 11.0 contains modified Weather Message and Emergency Override GUI software that checks the Message Type Listening Area Override parameter when the Message Type is selected. If the parameter is set, the following message will be displayed in a pop-up window:

Listening Area/Zone Override option set for <Message Type>; Unable to modify predefined area values.

The Weather Message and Emergency Override windows will then be displayed with the Area Selection buttons grayed out, preventing the operator from modifying the Listening Areas. This modification was implemented as CRS patch 10.0.2.

14. **TTR 919: EO Attempts To Broadcast On Invalid Transmitter During Retrieve** – Emergency Override (EO) has the capability to retrieve a previously saved message for the purposes of broadcasting it live via EO. If its Message Type has the Listening Area Override parameter set, the software erroneously uses the transmitter mapping of the retrieved message rather than that set by the default Listening Areas defined in the Message Type.

No users of the EO Retrieve option have been defined. Therefore, effective with CRS Build 11.0, the EO Retrieve option is non-operational.

15. **TTR 920: SSO Ignores LAC Override** – Synthetic Speech Override (SSO) was designed to allow sites to take advantage of the message parameters on incoming AWIPS messages, while allowing sites to manually record the message while the text is displayed on the operator's terminal. One of the options from the SSO window is "Transmit", which replicates the EO function, i.e. the message is transmitted live. For the SSO Transmit option, the software ignores Listening Area Override and uses the transmitter mapping of the incoming message rather than that set by the default Listening Areas defined in the Message Type.

No users of the SSO Transmit option have been defined. Therefore, effective with CRS Build 11.0, the SSO Transmit option is non-operational.

16. **TTR 921: Emergency Override (EO) Retrieve Message From Diskette Option Not Functioning** – A sub-option of the EO Retrieve capability is to retrieve the message from a diskette. This option does not function.

No users of the EO Retrieve option have been defined. Therefore, effective with CRS Build 11.0, the EO Retrieve option is non-operational.

17. **TTR 922: Null Default Areas Allowed For LAC Override** – Prior to CRS Build 11.0, operators were allowed to select Listening Area Override in the Message Type Window even if no default Listening Areas were selected. This would allow a message to be created with no assigned transmitters.

CRS Build 11.0 forces the operator to select default Listening Areas if the Listening Area Override option is selected.

18. **TTR 925: <u>Check AWIPS Interface Timeout</u>** – At system initialization and every 30 minutes thereafter, the software pings an AWIPS processor to ensure the AWIPS/CRS interface is operational. If the AWIPS processor does not respond within the ping timeout, the software will assume the AWIPS processor is not operational and will ping the next AWIPS processor in the **CRS_config.xml** file. Prior to Build 11.0, the ping timeout was 1 second, which is too short. If there were heavy system activity, this could cause the traversal of the entire set of AWIPS nodes without a successful ping. This would result in the generation of a spurious error message that the AWIPS interface was down. See TTR 926.

    CRS Build 11.0 changes the ping timeout to be the same as the ping timeout for AWIPS messages being sent to CRS.

19. **TTR 926: <u>Invalid Check AWIPS Interface Logic</u>** – Prior to Build 11.0, the logic that loops through the set of AWIPS nodes contained a logic error. If it loops through all six nodes without a successful ping, it will not generate the correct message indicating the AWIPS interface is down.

    CRS Build 11.0 corrects the logic error so that a failed AWIPS interface generates the correct error message.

20. **TTR 927: <u>Time Synchronization With AWIPS</u>** – All sites should be running with a configuration that runs Netsync once a day to retrieve the date/time from AWIPS and send it over the LAN to the shadow MP and FEPs. Netsync uses rdate to retrieve the current time from the "active" AWIPS processor contained in the configuration and previously determined during AWIPS connectivity checking done by CP_AI (see TTR 911). Prior to CRS Build 11.0, if rdate was unsuccessful, a successful error code was always returned. Therefore, if no date/time was returned from AWIPS, no indication of any problem was returned. The implementation of TTR 911 in patch 10.0.1 meant that normally the first AWIPS processor found during connectivity checking PX1. Neither PX1, PX2, DX1, nor DX2 support rdate. Therefore, normally sites would not be able successfully synchronize their time with AWIPS, and would not receive any indication of a problem via an Alert Monitor message or any other type of error message. This could have resulted in a time drift of the CRS MPs and FEPs over time.

    An optional workaround was distributed via CRS Technical Information Packet (TIP) that allowed sites to re-prioritize the AWIPS processors in the AWIPS Authorization file, so that DS1 and DS2 are checked first during AWIPS connectivity checking. Since both DS1 and DS2 support rdate, this would allow sites to time synchronize with AWIPS once again. AWIPS software changes planned for OB7.1 will activate rdate support on at least the DX platforms. (OB7 is the planned timeframe for the removal of the DS platforms.)

    CRS Build 11.0 modifies Netsync to call CP_AI to check the AWIPS interface. This allows Netsync to "use" the AWIPS processor checking logic to look for all 6 AWIPS platforms listed in the AWIPS Authorization file. Additional logic has been added to not only ping the

AWIPS processors, but to specifically ping port 37 that is used to determine if rdate is supported. Therefore, the AWIPS processor checking logic in CP_AI will continue looking for an AWIPS processor until it finds one that supports rdate. If it never finds an AWIPS processor that supports rdate, it will generate an alert monitor message that time synchronization is unavailable.

21. **TTR 931: Turn Off Password Aging** – Automatic 90-day password aging was added to the CRS and VIP software capabilities in the CRS Build 10.0/VIP Build 3.1 implementation. Potential problems with the crs user password expiration and subsequent failure to transfer messages from AWIPS to CRS lead to its **manual** removal in Software Note 7. CRS Build 11.0 removes the password aging mechanism permanently.

22. **TTR 934: GUI2ASCII Places "???" in Block 11 Replace TypeList and Block 12 Follow TypeList for Deleted Message Types** - Assume Message Type X is defined in the Message Type Association window to replace Message Type Y. That is, in BLOCK 11 of the .ASC file, X is the Message Type and Y is in the Replace TypeList. The intent of this is if X and Y messages have the same list of Listening Areas/Xones, X will replace Y in the broadcast schedule. The problem occurs if at some later time, Y is deleted from the list of Message Types (BLOCK 10). Even though the Message Type Association window will no longer display Y in the Replace TypeList, if you run the GUI2ASCII utility to generate a .ASC file from the stored database, it will generate "???" in place of Message Type Y in the .ASC BLOCK 11 Replace TypeList. This will cause a failure if you try to load the .ASC file into the database using the crs_site utility. The output from GUI2ASCII indicates that BLOCK 11 is creating "???". The workaround for this problem is to delete the Message Type from the Message Type Association window before deleting it from the Message Type window. The same problem occurs if you delete a Message Type that is listed in a FollowList (BLOCK 12) in the Message Type Association window.

This situation is analogous to deleting a Message Type without first deleting it from the Broadcast Suite. In this case, it automatically gets deleted from the suite as well, and there is no problem when GUI2ASCII generates the .ASC file. However, there must be some non-displayable character(s) left over in the Message TypeReplace list in the Message Type Association window that GUI2ASCII translates to "???".

In CRS Build 11.0, the GUI2ASCII software has been modified to not generate the "???" sequence in BLOCKS 11 and 12. Instead it will generate the following output error messages for BLOCKS 11 and 12 respectively:

Unable to add <Message Type ID> to the Message Type - Block 11 Replacement list for CCCNNNXXX

Unable to add <Message Type ID> to the Message Type - Block 12 Follow list for CCCNNNXXX

23. **TTR 948: CRS_SITE Limits Triggers In A Program To 127** – The crs_site software that loads the database from an ASCII database text file hangs when encountering more than 127 triggers in a specific program. This could prevent sites with a large number of triggers from being able to recover from a database failure. The CRS operational software allows sites to enter a virtually limitless number (32,767) of triggers in a program.

    CRS Build 11.0 modifies crs_site to explicitly checks for the number of triggers in a program and limits it to 32,767.

24. **TTR 950: DB_MH Fails –** Intermittently and without any consistency, db_mh, the database message handler, will fail and cause crs to stop and restart. This problem will occur when memory is deallocated and returned to the system if the necessary address needed to deallocate is overwritten due to a buffer overflow.

    CRS Build 11.0 modifies db_mh string functions to guarantee that only the allowed size of data is transferred from variable to variable, thereby reducing the risk of buffer overflows.

25. **TTR 953: CP_AI Memory Leak –** The AWIPS message input process, cp_ai, has a memory leak when it checks for the AWIPS interface.

    CRS Build 11.0 modifies the function that deallocates the memory used to check for AWIPS ip addresses and node names. It will properly deallocate the pointer to the pool of valid AWIPS nodes.

BUG FIXES – VIP

1. **TTR 817: VIP Timeouts From 4:00 – 4:30 System Time On VIP** – Prior to VIP Build 3.2, sites intermittently could see messages time out during the VIP conversion of text to speech between the hours of 04:00 – 4:30 system time. The daily house keeping cron jobs were scheduled to run at 04:02. The weekly house keeping cron jobs were scheduled to run at 04:22. The monthly house keeping cron jobs were scheduled to run at 04:42. The execution of these jobs causes a slowdown of the VIP, thereby causing an increase in the time necessary to convert a VIP message from text to speech. It could be enough of a delay to cause the conversion to not complete in the maximum time allotted of 60 seconds.

   VIP Build 3.2 reschedules the weekly cron jobs to run at 05:22 and the monthly to 06:42.

2. **TTR 829: Non-Spanish VIP Installation Does Not Check For Spanish Messages** – There are only 14 Spanish licenses available to be used among operational CRS sites. However, Prior to VIP Build 3.2, the VIP software always had the Spanish text-to-speech (tts) server

running along with the other two English tts servers. The VIP software did not check the table of Spanish license site identifiers for authorized users. Therefore, even if a site did have an assigned and authorized Spanish license to use, Spanish text messages could be successfully converted to voice in the VIP.

VIP Build 3.2 has added new logic to the Setup Wizard GUI to save a flag when a non-Spanish site is detected during the setup and to not run the Spanish tts server if the flag is present. If a non-licensed site receives a VIP Spanish text message, the VIP will display an error message: **Spanish Conversion Not Permitted**. And the message will default to Spanish DECTalk voicing. Effective with VIP Build 3.2, Corpus Christi has been added to the approved list of Spanish licenses.

3. **TTR 895: VIP Scrubber Process Does Not Run If VIP Server Is Restarted Frequently (Less Than 12 Hours Apart)** – The VIP scrubber routine cleans out the directories containing the VIP voice files, including the CRS .Pv files and the remote sftp .wav and .mp3 files. Since the subdirectories containing these files are in the root partition, failure of the scrubber process will ultimately cause the root partition to fill up and crash the VIP.

   The scrubber process is initiated by the VIP server process. Prior to VIP Build 3.2, when the VIP sever process was started, it instructed the scrubber to sleep for 12 hours and then start. If the VIP application was restarted during that time, clock was effectively restarted, and the scrubber never ran.

   Effective with VIP Build 3.2, the scrubber routine is scheduled to run when the VIP server process is started and every 12 hours thereafter.

4. **TTR 896: Need A Cron Job To Periodically Remove Old Maintenance And Runtime Logs From VIP** – Various logs of VIP application activity are stored on the VIP to aid in debugging problems. Keeping a month worth of activity is sufficient length to aid in the debugging activity. However, if left to accumulate indefinitely, it is possible to fill up the root partition and crash the VIP. Prior to VIP Build 3.2, the logs were removed only when a new disk image was restored to load new software.

   VIP Build 3.2 contains a new script, VIPCleanLog, which runs once a month to delete log files more than a month old.

5. **TTR 899: VIP GUI Stops Running** – The VIP software will deliberately shut itself down by killing the GUI main interface when certain errors are encountered. The VIP application will stop running when the following errors occur:

   - Fail to read the VIP.env file.
   - Fail to create a thread.
   - Fail to create a CRS audio file.
   - Fail to read a dictionary file.

- Fail to convert text to speech from the calling functions in the text-to-speech library.
- Fail to communicate with the CRS Master MP for over 4 minutes, which could happen during the MP switch process.

Prior to VIP Build 3.2, the operator received no notification indicating the reason for the VIP application termination.

VIP Build 3.2 contains new popup dialog boxes that display appropriate error messages describing the reason for the VIP shutdown.

6. **TTR 904: VIP SFTP Of Converted .WAV Files Back To Master MP Is Considerably Slower Than FTP** – Prior to VIP Build 3.2, transfer rates of complete voice files back to the Master MP from the sftp in the VIP Perl Script (DataTransfer) were considerably slower compared to those from the old ftp version. This could cause larger messages to time out, which would result in the broadcast of those messages with the old DECTalk voice and prevent sites using the remote sftp function from delivering the .wav or .mp3 to the remote system.

   VIP Build 3.2 contains a new Bash script with embedded sftp commands, which allows the sftp commands to run in batch mode rather than interactive mode. The embedded sftp commands results in transfer rates similar to the previous ftp commands.

7. **TTR 907: Need To Remove Password From VIP.env on VIP** – Prior to VIP Build 3.1, the crs user password was included in the VIP.env file. It was necessary to include when configuring the System Setting GUI and the optional Audio FTP Configuration GUI. However, with implementation of sftp to replace ftp in VIP Build 3.1, the utilization of the crs password for these functions became unnecessary.

   The VIP Build 3.1 software removes the password field from the VIP.env file and no longer requires entering it in the System Setting GUI, the Audio FTP Configuration GUI, or the Setup Wizard GUIs for these same functions.

8. **TTR 915: Add Progeny Security Patches To Red Hat 7.3 OS** – VIP Build 3.1 includes the Progeny security patches to Red Hat Linux 7.3.

9. **TTR 917: Add New Key West Site Identifier to VIP** - The Key West office is moving to another location on the island, which requires changing the site identifier from KEYW to KKEY. The WFOsites.env file has been changed to add KKEY to the file.